S E C R E T MOSCOW 001238

SIPDIS

S/CT FOR HILLARY BATJER JOHNSON AND PAUL SCHULTZ

E.O. 12958: DECL: 05/14/2019
TAGS: KVPR PTER PREL PGOV CVIS ASEC KHLS RS
SUBJECT: RUSSIA: UPDATES ON COLLECTION, SCREENING, AND
SHARING BORDER CONTROL INFORMATION

REF: STATE 32287

Classified By: Political M/C Alice G. Wells for reasons 1.4 (b), (c), a
nd (d).

¶1. (C) Post responses are keyed to reftel questions. Please
note that the working relationship between the USG and the
Russian Federation is difficult and there is little
information sharing outside of specific cases. Much of the
information that follows is anecdotal, based on the Embassy's
experience, or from publicly available literature. Not all
regulations and procedures are available to us, as some are
classified or in restricted distribution.

¶2. (SBU) A. Immigration Databases and Traveler Information
Collection:
-- (SBU) Q. What computerized databases are used to track
entries and exits? A. The Federal Border Guard Service
(FBGS) under the Federal Security Service (FSB) maintains and
operates the country's database. The database collects name,
purpose of travel, itinerary, along with relevant passport
and visa information.

-- (SBU) Q. Is the computerized immigration database
available at all ports of entry (POEs)? A. Terminals are
located at major Russian ports of entry, but not all.

-- (SBU) Q. If immigration databases are available at some
POEs, but not all, how does the host government decide which
POEs will receive the tool? A. We have little information
on the decision process, but speculate that it depends on
immigrant flow, financial resources available, political
context, and potential threats identified as coming from a
specific source.

-- (SBU) Q. What problems, if any, limit the effectiveness
of the systems? For example, limited training, power
brownouts, budgetary restraints, corruption, etc...? A.
Informally, we have heard that budget constraints have
limited the effectiveness of the system but without any
specifics as to how or why.

-- (SBU) Q. How often are national immigration databases
updated? A. Unknown.

-- (SBU) Q. What are the country's policies (legislation,
mandates, etc...) on collecting information from travelers
arriving in the country? A. The principal piece of
legislation is the Federal Act on Exit/Entry Procedures
(FAEEP), as amended, in force since July 18, 1996. The FBGS
complies with this law and the implementing procedures, many
of which are classified. Art. 6 of the FAEEP states that
foreign citizens and stateless persons must produce a valid
ID document, recognized by the Russian Federation, and a visa

when entering/exiting Russian Federation territory, unless
otherwise stated by federal law, presidential decree, or
treaty. International carriers are obligated under this law
to verify the person traveling has a valid visa or other
permit.

-- (SBU) Q. Are there different polices for entry and exit
at air, sea, and land POEs and for domestic flights? A. Yes.

-- (SBU) Q. What agency oversees the collection of traveler
information? A. The Federal Migration Service is charged
with maintaining information on persons traveling and
residing within Russia, and the FBGS/FSB maintains records on
persons traveling into and out of Russia.

-- (SBU) Q. What are the policies of the collecting agency
to share that information with foreign governments? A.
These policies are based upon bilateral treaties, and a
release of information may be authorized in response to a
formal diplomatic request but on a case-by-case basis. In a
criminal case, Russia will share information through Interpol
channels.

-- (SBU) Q. Does the host government collect Passenger Name
Record (PNR) data on incoming commercial flights or vessels?
¶A. Yes.

-- (SBU) Q. Is this data used for intelligence or law
enforcement purposes to screen travelers in a systematic way?
 ¶A. Unknown.

-- (SBU) Q. Does the host government have any existing
treaties to share PNR data? A. Russia and the U.S. signed a

Mutual Legal Assistance Treaty, ratified November 3, 2000,
and under Article 2 provides a general agreement that may
permit the sharing of PNR data in individual cases: "Legal
assistance under this Treaty shall include ... providing any
other legal assistance not prohibited by the laws of the
Requested Party."

-- (SBU) Q. If applicable, have advance passenger
information systems (APIS), interactive advanced passenger
information systems (IAPIS) or electronic travel authority
systems been effective at detecting other national security
threats, such as wanted criminals? A. Unknown.

¶3. (SBU) B. Watchlisting:
-- (SBU) Q. Is there a name-based watchlist system used to
screen travelers at POEs? A. Yes.

-- (SBU) Q. What domestic sources of information populate
the name-based watchlist, i.e., names of deported persons,
terrorist lookouts, criminal want/warrants? A. Contributors
include Ministry of the Interior, FSB, General Prosecutor's
Office, and Ministry of Justice (service equivalent to the
U.S. Marshals Service).

-- (SBU) Q. If the host government maintains a watchlist,
how many records does the watchlist contain, and how many are
terrorist-related? A. Unknown.

-- (SBU) Q. Which ministry or office maintains the
watchlist? A. The principal list used for entry/exit is
maintained by the FSB, but the Ministry of the Interior,
General Prosecutor's Office, and Ministry of Justice maintain
additional lists.

-- (SBU) Q. What international watchlists do the host
government use for screening individuals, e.g., Interpol or
TSA No Fly lists, UN, etc...? A. International airlines
operating into and out of Russia utilize the TSA
watch-listing system. The GOR also uses Interpol and UN
lists.

-- (SBU) Q. What bilateral/multilateral watchlist agreements
exist between the host government and its neighbors? A. The
full extent of bilateral and multilateral agreements is

unknown. However, Russia signed an agreement with
Commonwealth of Independents States (CIS) members in 1993 on
legal assistance; joined UN conventions including Convention
on Drug Trafficking and Psychotropic Substances Control
(December 20, 1988), International Convention on Terrorism
Financing Control (December 9, 1999), Convention Against
Transnational Organized Crime (November 15, 2000); and joined
the European Convention on Extradition (December 13, 1957)
and the European Convention on Mutual Legal Assistance (1959).

¶4. (SBU) Biometrics:
-- (SBU) Q. Are biometric systems in place at ports of entry
(air, land, and sea)? A. Yes.

-- (SBU) Q. If biometric systems are available at some POEs,
but not all, how does the host government decide what POEs
will receive the tool? A. Unknown.

-- (SBU) Q. What biometric technologies, if any, does the
host government use, i.e., fingerprint identification, facial
recognition, iris recognition, hand geometry, retinal
identification, DNA-based identification, keystroke dynamics,
gait analysis? A. Russia maintains a database of Russian
citizen photographs which is in place and utilized at some
major ports of entry into and out of Russia. Post is aware
of GOR plans to install fingerprint identification systems at
major POEs, but we do not have any details.

-- (SBU) Q. Are the systems ICAO compliant? A. Unknown.

-- (SBU) Q. Are biometric systems integrated for all active
POEs? A. No.

-- (SBU) Q. What are the systems and models used? A.
Unknown.

-- (SBU) Q. Are all passengers screened for the biometric or
does the host government target a specific population of
collection (i.e., host country nationals)? A. Unknown.

-- (SBU) Q. Do the biometric collection systems look for a
one to one comparison (ensure the biometric presented matches
the one stored on the e-Passport) or one to many comparison

(checking the biometric presented against a database of known
biometrics)? A. The existing database is used for matching
the document to the data (one to one) at the POE.

-- (SBU) Q. If biometric systems are in place, does the host
government know of any countermeasures that have been used or
attempted to defeat biometric checkpoints? A. It is known
that standard fraud practices, such as visa and passport
photo-substitution, are common at international airports in
Russia. Countermeasures are unknown.

-- (SBU) Q. What are the host government's policies on
collecting fingerprints of travelers coming into the country?
 ¶A. Travelers fingerprints are not presently collected as a
matter of course, although a traveler may be printed if he
has committed a criminal offense.

¶5. (SBU) Border Control and Screening:
-- (SBU) Q. Does the host government employ software to
screen travelers of security interest? A. Software is used
to track travelers (including domestic flights and trains)
Russia-wide for law enforcement purposes.

-- (SBU) Q. Are all travelers tracked electronically, or
only non-host country nationals? A. Russia maintains both
an internal and external travel documentation system and a
Russian citizen must have an internal passport and an
external passport to travel within and without the country.
Entry and exit records are maintained for travelers through
major POEs; however, non-recorded entries may occur,
especially when a traveler arrives from a CIS country by
train or by car.

-- (SBU) Q. What is the frequency of travelers being "waved

through" because they hold up what appears to be an appropriate document, but whose information is not actually recorded electronically? A. At many ports of entry into and out of Russia, visual inspection of documentation appears to be the only system used for admitting persons for entry and exit. For example, at some ports persons present their document, it is visually inspected, and the person is waved through.

-- (SBU) Q. What is the estimated percentage of non-recorded crossings, entries and exits? A. Unknown.

-- (SBU) Q. Do host government border control officials have the authority to use other criminal data when making decisions on who can enter the country? If so, please describe this authority (legislation, mandates, etc...). A. Articles 26 and 27 of the FAEEP specifies who may not be allowed to enter the Russian Federation and under what legal grounds. The FBGS has the authority to use criminal or other data. Police services may also intervene in the process.

-- (SBU) Q. What are the host government's policies on questioning, detaining and denying entry to individuals presenting themselves at a point of entry into the country? ¶A. Articles 26 and 27 of the FAEEP provide legal basis. Post does not have access to the implementing policies and procedures.

-- (SBU) Q. Which agency would question, detain, or deny entry? A. The FBGS and FSB.

-- (SBU) Q. How well does information sharing function within the host government, i.e., if there is a determination that someone with a valid host-government visa is later identified with terrorism, how is this communicated and resolved internally? A. Unknown.

¶5. (SBU) E. Passports:
-- (SBU) Q. Does the host government issue a machine-readable passport containing biometric information? If so, what biometric information is included on the document, i.e., fingerprint, iris, facial recognition, etc...? A. Yes. A bearer's photograph, date of birth, place of birth, place and date of document issuance, and agency of issuance. Both the Ministry of Foreign Affairs and the Federal Migration Service issue passports in Russia.

-- (SBU) Q. If the host government issues a machine-readable passport containing biometric information, does the host government share the public key required to read the biometric information with any other governments? If so, which governments? A. The biometric information is printed on the document, a public key is not required.

-- (SBU) Q. Does the host government issue replacement passports for full or limited validity (i.e., the time remaining on the original passports, fixed validity for a replacement, etc...)? A. Russian passports, including replacements are issued for a period of five years. Russian nationals can carry two valid passports at the same time, with the same expiration date.

-- (SBU) Q. Does the host government have special regulations/procedures for dealing with "habitual" losers of passports or bearers who have reported the passports stolen multiple times? A. "Habitual" losers may have an administrative fine imposed on them or a record with the local police.

-- (SBU) Q. Are replacement passports of the same or different appearance and page length as regular passports (do they have something along the lines of our emergency, partial duration passports)? A. No, although Russian consulates can issue a special certificate to enable a national to return to Russia (similar to our transportation letters).

-- (SBU) Q. Do emergency replacement passports contain the

same or fewer biometric fields as regular-issue passports?
¶A.   There is no specific emergency passport.

-- (SBU) Q. Where applicable, has Post noticed any increase
in the number of replacement or "clean" (i.e., no evidence of
prior travel) passports used to apply for U.S. visas? A. No.

-- (SBU) Q. Are replacement passports assigned a
characteristic number series or otherwise identified? A. No.

¶6. (SBU) F. Fraud Detection:
-- (SBU) Q. How robust is fraud detection and how actively
are instances of fraud involving documents followed up? A.
Unknown. Attempts by DHS/ICE to share information with
Russian migration authorities have been unsuccessful to date.

-- (SBU) Q. How are potentially fraudulently issued
documents taken out of circulation, or made harder to use?
¶A.   The Federal Migration Service issues lists of passports
declared null and void.

¶7. (SBU) G. Privacy and Data Security:
-- (SBU) Q. What are the country's policies on records
related to the questioning, detention or removal of
individuals encountered at points of entry into the country?
¶A. Record handling procedures depend on the nature of the
incident. If the incident was criminal in nature,
record-keeping would follow the provisions of the Criminal
Procedure Code.

-- (SBU) Q. How are those records stored, and for how long?
¶A. Unknown, although some of the records are covered under
the Federal Law on Information Technologies and Data
Protection (July 27, 2006).

-- (SBU) Q. What are the country's restrictions on the
collection or use of sensitive data? A. Unknown, although
partially covered under the Federal Law on Information
Technologies and Data Protection (July 27, 2006).

-- (SBU) Q. What are the requirements to provide notice to
the public on the implementation of new databases of records?
 ¶A. Unknown, although some of the records are covered under
the Federal Law on Information Technologies and Data
Protection (July 27, 2006).

-- (SBU) Q. Are there any laws relating to security features
for government computer systems that hold personally
identifying information? A. Unknown, although some of the
records are covered under the Federal Law on Information
Technologies and Data Protection (July 27, 2006).

-- (SBU) Q. What are the rules on an individual's ability to
access data that homeland security agencies hold about
them? A. Unknown, although some of the records are covered
under the Federal Law on Information Technologies and Data
Protection (July 27, 2006).

-- (SBU) Q. Are there different rules for raw data (name,
date of birth, etc.) versus case files (for example, records
about enforcement actions)? A. Unknown, although some of
the records are covered under the Federal Law on Information
Technologies and Data Protection (July 27, 2006).

-- (SBU) Q. Does a non-citizen/resident have the right to
sue the government to obtain these types of data? A.
Article 17 of the Russian Federation Constitution recognizes
and guarantees the human rights and freedoms of
non-citizens/residents while staying in Russia, including the
right to sue the government. While a right, this is
difficult in practice.

¶8. (SBU) H. Identifying Appropriate Partners:

-- (SBU) Q. Department would appreciate Post's in-house
assessment of whether host government would be an appropriate
partner in data sharing. Considerations include whether host

government watchlists may include political dissidents (as opposed or in addition to terrorists), and whether host governments would share or use U.S. watchlist data inappropriately, etc.... A. Russia's system of entry/exit controls is highly secretive and opaque with little demonstrated interest in improved cooperation. We will continue to seek opportunities for cooperation, and LEGAT has a pending offer to share NCIC data with the FSB.

-- (S) Q. Are there political realities which would preclude a country from entering into a formal data-sharing agreement with the U.S.? A. Russia poses a significant intelligence threat to official U.S. personnel and to American citizens. The FSB, which presents much of that threat, controls the data to which we would seek access.

-- (SBU) Q. Is the host country's legal system sufficiently developed to adequately provide safeguards for the protection and nondisclosure of information? A. The GOR is well-versed in non-disclosure and can certainly safeguard information from unintended disclosure.

-- (SBU) Q. How much information sharing does the host country do internally? Is there a single consolidated database, for example? If not, do different ministries share information amongst themselves? A. Agencies maintain multiple databases and have historically not shared this information amongst themselves.

-- (SBU) Q. How does the country define terrorism? Are there legal statutes that do so? A. Article 3 of The Russian Federation Law on Counter Terrorism (Federal Law No. 35-F3) of March 6, 2006, as amended, states "Terrorism is an ideology of violence and a practice consisting of exercising an impact on decision-making government authorities, local government institutions or international organizations, this ideology and practice is connected to the intimidation of the population and/or other patterns of unlawful violent acts." However, Russia has also defined "extremism" which has been criticized for including acts of political opposition and civil disobedience.
RUBIN